# Intelligence after Intellipedia: Improving the Push Pull Balance with a Social Networking Utility

by
 Ariane Ben Eli and Jeremy Hutchins
 Pratt Institute
 School of Information and Library Science

**Approved for public release; distribution is unlimited.**

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| 1. REPORT DATE *(DD-MM-YYYY)* 08-02-2010 | 2. REPORT TYPE Research Report | 3. DATES COVERED *(From - To)* | |
|---|---|---|---|
| **4. TITLE AND SUBTITLE** Intelligence after Intellipedia: Improving the Push Pull Balance with a Social Networking Utility | | **5a. CONTRACT NUMBER** | |
| | | **5b. GRANT NUMBER** | |
| | | **5c. PROGRAM ELEMENT NUMBER** | |
| **6. AUTHOR(S)** Ben Eli, Ariane Hutchins, Jeremy | | **5d. PROJECT NUMBER** | |
| | | **5e. TASK NUMBER** | |
| | | **5f. WORK UNIT NUMBER** | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Pratt Institute School of Information and Library Science | | **8. PERFORMING ORGANIZATION REPORT NUMBER** | |
| **9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)** Defense Technical Information Center 8725 John J. Kingman Road, Suite 0944 Fort Belvoir, VA 22060-6218 | | **10. SPONSOR/MONITOR'S ACRONYM(S)** DTIC-E | |
| | | **11. SPONSOR/MONITOR'S REPORT NUMBER(S)** TR-2010/05 | |

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Approved for public release; distribution is unlimited.

**13. SUPPLEMENTARY NOTES**
Winner of DTIC's 2010 Student Paper Competition. Included in DTIC-E-TR-2010/04. Copyright ©2010 (A. Ben Eli and J. Hutchins). The U.S. Government and those authorized on its behalf are granted an unlimited non-exclusive, royalty-free, world-wide license to use, reproduce, or release the work for U.S. Government purposes.

**14. ABSTRACT**
In response to the terror threat following September 11, 2001, the United States set up an intelligence hub to aggregate and analyze data and intelligence produced by the 16 agencies and departments that make up the Intelligence Community. The hub, first called the Terrorist Threat Integration Center and succeeded by the National Counterterrorism Center, collaborates with foreign allies and draws on at least thirty databases to track threats and determine the credibility of intelligence. There is now no shortage of data and information to be turned into intelligence; the new challenge lies in convincing agencies to truly cooperate to reach national security goals. This paper seeks to study various approaches for increasing cooperative problem solving by examining existing tools. It proposes better knowledge management through the implementation of database comparison tools within an online social network to encourage new, dynamic intelligence cooperation that connects the dots between isolated items of intelligence and thus makes intelligence more timely and actionable.

**15. SUBJECT TERMS**
Social networking, Intellipedia, 2010 Student Paper Competition

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON Carol E. Jacobson |
|---|---|---|---|---|---|
| **a. REPORT** Unclassified | **b. ABSTRACT** Unclassified | **c. THIS PAGE** Unclassified | UU | 13 | **19b. TELEPHONE NUMBER** *(include area code)* 703-767-9167 |

**Standard Form 298 (Rev. 8-98)**
Prescribed by ANSI Std. Z39.18

Defense Technical Information Center
Student Paper Competition
2010 Conference

Author Names:          Jeremy Hutchins
                       jhutchin@pratt.edu
                       (917) 374-0723

                       Ariane Ben Eli
                       abeneli@pratt.edu
                       (917) 892-4706

School Affiliation:    Pratt Institute
                       School of Information & Library Science
                       144 West Fourteenth Street
                       New York, NY 10013

Department chair:      Dean Tula Giannini, Ph.D., MLS, MM
                       giannini@pratt.edu

Title:  **Intelligence after Intellipedia: Improving the Push Pull Balance with a Social Networking Utility**

*Abstract:*

*In response to the terror threat following September 11, 2001, the United States set up an intelligence hub to aggregate, assess and analyze data and intelligence produced by the 16 agencies and departments that make up the Intelligence Community. The hub, first called the Terrorist Threat Integration Center and succeeded by the National Counterterrorism Center, collaborates with foreign allies and draws on at least thirty databases to track threats and determine the credibility of intelligence. There is now no shortage of data and information to be turned into intelligence; the new challenge lies in convincing agencies to truly cooperate to reach national security goals. This paper seeks to study various approaches for increasing cooperative problem solving by examining existing tools. It proposes better knowledge management through the implementation of database comparison tools within an online social network to encourage new, dynamic intelligence cooperation that connects the dots between isolated items of intelligence and thus makes intelligence more timely and actionable.*

*Introduction:*

Following the attacks of September 11, 2001, the United States intelligence community took steps to increase collaboration between all parts of the government to apprehend terrorists and prevent future attacks. This new whole-of-government approach was embodied in the creation of the National Counterterrorism Center (NCTC) in 2004. The NCTC would act as a hub, with analysts from the 16 intelligence agencies working side by side, sharing networks, databases, and information. When actionable intelligence emerged, the NCTC, through its Interagency Threat Assessment and Coordination Group (ITACG) would be able to communicate with state, local, tribal and federal law enforcement to respond in near real-time to threats as they emerged.

## A First Step: Creating the Intelligence Hub

The NCTC's online digital library, NCTC Online (NOL) would enable access to intelligence agencies' networks and websites. A 2006 internal report card indicated that NOL hosted over 6,000 users and 6 million documents from over 60 contributing departments and agencies. Its identified user groups included the Terrorist Screening Center, National Security Agency, Defense Intelligence Agency, Department of Homeland Security, State Department, Daily News Update of the Department of Defense, Department of Defense, Federal Bureau of Investigation and the Central Intelligence Agency. In his statement for the record before the House Homeland Security Committee's Sub-Committee on Intelligence, Information Sharing and Terrorism dated 13 March 2008, Michael Leiter, then Acting Director of the NCTC said,

> "I cannot overstate the importance of NCTC Online Secret (NOL(S)). From my perspective, NOL(S)--a secure, classified website designed to mirror the Top Secret version that is used broadly by federal officials--is a, if not the, key access point to counterterrorism information for SLT...we must increase the utility of NOL(S) as well as increase SLT awareness of NOL(S)...We are working with our federal partners...to ensure an even richer data set. This will include reporting related to breaking events, daily terrorism related situational reports, as well as an array of foundational reports..."

Elsewhere, NOL(S) is described as a vast data warehouse, drawing from not just the intelligence community, but public records, the Department of Agriculture, the Bureau of Alcohol, Tobacco, Firearms and Explosives, police departments, Commerce, Energy, the Federal Aviation Administration, the Department of Transportation, the Federal Reserve and others. Until at least 2008, the resource gave users access to CIASource and SIPRNet, the Defense Department's communications backbone, used for passing tactical and operational information at the secret classification level.

The goal of the NCTC was to aggregate, integrate, analyze and effectively disseminate actionable intelligence to the appropriate users rapidly. One challenge for the agency, from the beginning, was asserting its authority of agencies and departments with their own established hierarchies, leadership, and goals. The FBI was not eager to share everything with the CIA, DIA or anyone else and vice versa.

Getting the various arms of the intelligence community to work together was a high priority at the NCTC. In fact, its publicly accessible webpage trumpets that "collaboration is one of our best weapons against terrorism"[1] In its promotional video, the NCTC describes itself as "the central and shared knowledge bank of all known and suspected terrorists and international terrorist groups." The creation of intelligence hubs to aggregate data and information and to facilitate what was commonly called collaboration before 2009 may have been seen as a way to increase efficiency when responding to current and emerging security threats.[2]

### Intellipedia as a Collaborative Intelligence Tool

In 2006, the United States intelligence community announced its new tool, *Intellipedia*, a wiki and blog network for its 16 agencies and departments to share information and collaborate on intelligence products. By most accounts, the project has been a useful tool for the agencies and departments that actually use it. Because users are not anonymous, they have a stake in being accurate and honest. When users input inaccuracies, other members of the community rapidly correct them.

*Intellipedia* grew out of a 2004 paper authored by D. Calvin Adrus, entitled "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," which proposed that US policymakers, war-fighters and law-enforcers must learn to operate in a security environments that is changing rapidly in ways they cannot predict.

"The only way to meet the continuously unpredictable challenges ahead of us is to match them with continuously unpredictable changes of our own," he wrote. Basing his proposal on six elements of complexity theory that he outlined, he suggested that a wiki—a community organized, collaborative encyclopedia, which could be edited by any user, and which allows free flowing comments and discussion—would behave as a self-organizing tool for the intelligence community.

In describing *Wikipedia*, the most well known of several wiki websites, Adrus wrote, "from little bits of work by many, many people following simple rules of content contribution and editing, the most comprehensive, authoritative, and bias-free encyclopedia in the world has been produced in four years. This is an encyclopedia that is dynamically and constantly changing in response to the world as the world itself is changing." In describing how a wiki

---

[1] from NCTC video transcript available at http://www.nctc.gov/docs/nctc-video-transcript.pdf, and accessed 2/5/2010 13:58:00

[2] Whether hubs actually result in greater efficiency is debatable. In November 2008, Google Flu Trends reported it could accurately predict flu outbreaks between seven and 14 days earlier than the Federal Centers for Disease Control and Prevention based on Google users' search terms and geographical locations. See http://www.google.org/flutrends/.

The reason given was that people would search for their symptoms online before visiting a healthcare provider, while the CDC relied on reports from healthcare providers to make its own forecasts.

could work for the intelligence community, Adrus suggested that "A healthy market of debatable ideas emerges from the sharing of points of view. From the ideas that prosper in a market will arise the adaptive behaviors the Intelligence Community must adopt in order to respond to the changing national security environment."

Andrus' paper was published in 2005. By the end of the year, a pilot program had begun to create *Intellipedia*, and it was formally announced in the fall of 2006. In the six months from April to October of that year, *Intellipedia* had already grown to 28,000 pages and had 3, 600 users, according to news reports. By the fall of 2009, the site was home to 900,000 pages and had 100,000 registered users. It averaged over 15,000 page edits a day.

*Intellipedia* as an idea perfectly coalesced with the collaborative goals of the national security and intelligence communities at the time. Wikis by their very definition are collaborative, relying on the collective wisdom of the group for their timeliness, factually correctness and accuracy. Yet in early 2009, Chris Rasmussen, a social-software knowledge manager at the National Geospatial Intelligence Agency was quoted at length detailing some of the challenges *Intellipedia* had encountered. By Rasmussen's estimate in February 2009, "all those who would have joined and shared their knowledge on the social networking site have already done so." Further, few intelligence agencies had incorporated *Intellipedia* into their formal decision making process.[3]  Many agencies duplicated information, he said, using *Intellipedia* as a shadow system. "An agent may have had an informative conversation on *Intellipedia*, but then documents the exchange on some agency's official system as well, 'if you move the content and the conversation to the new space, why maintain the old?'" Rasmussen asks. To the authors of this paper, at least, the answer seems obvious: without *Intellipedia* the conversation wouldn't happen at all.

Despite these successes, the Defense Department's 2010 Quadrennial Defense Review calls for even greater cooperation. While the change from *collaboration* to *cooperation* may simply be semantics, this could signal a real change in policy. To understand the difference between *collaboration* and *cooperation*, one might think of a group of students at work at the same time. If the students are actively engaged in say, tagging a shared map of their city to identify streets, businesses, municipal buildings, schools, parks and places they have in some way claimed, they might be understood to be collaborating. The map they make relies on the input of everyone involved and is fundamentally changed by their participation. If, however, each student is engaged in making his or her own map but must share the tools and limited resources available with the other students at the table (and they achieve some balance and harmony in their tool sharing), they are better understood to be cooperating.

The authors believe that while collaboration is important, and has been shown to work with tools like *Intellipedia*, cooperation may be more feasible as a goal for the  intelligence community.  In her statement before the Council on Foreign Relations, Michele Flournoy, the undersecretary of defense for policy, said, "we need to emphasize cooperation more in

---

[3] "Intellipedia suffers midlife crisis." By Joab Jackson, *Government Computer News*, February 18, 2009, retrieved February 8, 2010 <http://gcn.com/Articles/2009/02/18/Intellipedia.aspx>

everything we do – to think more deeply about what our allies and partners abroad and civilian partners at home can bring to the table."[4]

While collaboration was achieved in large part by the introduction of technological tools, and while technological tools will play a large part in achieving greater cooperation, as well, knowledge management must be a first consideration when attempting to get agencies with valid security concerns, and the legacy of Cold War secrecy, to act cooperatively. One lesson of *Intellipedia* is that younger members of the intelligence community who are already more comfortable in a social networking environment are more likely to adopt such tools at work. Since many of the decision makers and high officials in the national security and intelligence communities are veterans of Cold War policies, it's the job of knowledge managers to show them how these new tools, greater cooperation, and less secrecy within the community will lead to real results—less data loss between agencies, better intelligence products, and real time response to national security situations, before they develop into life threatening events. To borrow from Rasmussen, if an FBI agent were writing a useful article about Fidel Castro but tagged it with an agency identification (FBI in this example) instead of identifying the substantive issues of his article, (Fidel Castro, Cuba, etc.), the information would be, for all intents and purposes, lost.

Unfortunately there has been a real problem with data loss during aggregation within the intelligence and defense communities.  On January 5, 2010, less than two weeks after Umar Farouk Abdulmutallab, a 23-year-old Nigerian terrorist who claimed affiliation with Al Qaeda, tried to blow up a Northwest Airlines jet on its approach to Detroit, President Barack Obama outlined a series of changes in security procedures aimed at making Americans less vulnerable to terror attacks. His announcement came after two hours of talks with the heads of 20 departments and agencies, including the CIA, FBI, DHS, and the National Counterterrorism Center.

"This was not a failure to collect intelligence, it was a failure to integrate and understand the intelligence that we already had," President Obama said.


### *Knowledge Management Prevents Information Loss*

Knowledge management gives organizations a series of tools to make decision makers smarter, faster. It seeks to shed light on what one might call the unknown knowns, knowledge that exists within an agency or department but is unacknowledged or poorly understood. In business, the idea that all sorts of valuable information such as customers'

---

[4] Prepared Remarks: Michèle Flournoy, Undersecretary of Defense for Policy, p. 11, Council on Foreign Relations, February 2, 2010

http://www.cfr.org/publication/21350/prepared_remarks.html

preferences or employees private knowledge – was simply disappearing into the cracks which separate teams and business units led to the emergence of knowledge management as a discipline. People within their silos could not or would not share knowledge. There was a lingering sense of unconnectedness, of dots still not being joined up.

*Intellipedia* has achieved some success in connecting dots. However, its shortcoming is that to a great extent it still operates as "pull intelligence;" that is to say, users within the system have to seek out information. In order to seek out information, someone has to have a reasonably good idea of what they are looking for. One of the challenges for knowledge managers, some of whom may come from a library background, is that posed by the basic reference interview—smart people frequently haven't narrowed down large topics into relevant questions. Someone writing a paper such as this one might begin with a topic as broad as counterterrorism itself. The job of the reference interview is to narrow the topic down enough to arrive at relevant results.

Pull intelligence is, of course, extremely valuable. It means that when a person asks for items related to a particular topic, they are able to get relevant information that broadens understanding, informs reports, opinions and ultimately decision-making. But to know what to pull, frequently people benefit from what is called push intelligence: the sort of intelligence that is offered without asking. This provides users with resources that also broaden their understanding, inform reports and opinions and ultimately decision making, but that the user might not find on their own, that might be totally relevant but not immediately obvious. What someone receives as push intelligence may influence what sort of intelligence they pull on their own.

Push intelligence may prevent data and information from slipping through the cracks, relevant intelligence from being ignored or lost, and it can also demonstrate the value of interagency cooperation. After 8 years of focused action to increase collaboration in the counterterrorism and defense communities, it seems reasonable to assume that the national security and intelligence community is awash in data. The challenge now is to make sure that data isn't lost, that it becomes intelligence, and that this intelligence is timely, accurate, actionable and acted upon. Now is the time for a new knowledge management approach.

Knowledge management is most effective when it gets people to talk to one another, to share ideas and bits of information, to be able, through cooperation to see previously unrecognized patterns, make hidden connections and correlate, and even fuse, intelligence as a result. By setting up an intelligence hub, the US government sought to create the environment in which this sort of confluence of ideas would flourish, where data and information would be transformed into actionable intelligence. But shared databases which permit users to enter comments, daily video conferences and frequent email between working groups do not automatically translate into rigorous fact following. In a blog post dated January 4, 2010 Harvard Business School's Rosabeth Moss Kanter said that dispatching e-mails or entering comments into databases is not enough. Only "relentless

follow-up" would hold colleagues accountable for what they were supposed to be doing. Ms. Kanter wrote:

> "To be meaningful, isolated pieces of information must be connected. The NW 253 debacle was preceded by missed signals and uncorrelated intelligence — however partial, incomplete, and non-obvious — as an unnamed federal official told New York Times reporters. But isn't non-obvious the point of secrets? If somebody stumbles upon a bit of information but works in isolation, he or she might not see its significance. In an era of social networking, instant messaging, and continual tweeting, it should be easy to encourage people to share and connect their data points to find patterns. Leaders should reward pattern-recognizers."

Ms. Kanter's remarks strike on something that may be achieved through a thoughtful combination of knowledge management technology solutions and applied human aptitude. There are tools which exist, including shared databases (both open source and classified), visualization software and geospatial imaging as well as civilian-created data such as personalized Google maps, news archives, blogs, and tweets. Might there be social networking solutions for making existing tools more useful in revealing hidden connections and in creating actionable intelligence?

### *Putting Social Networking to Work May Enable Cooperative Intelligence*

Facebook, by far the most popular social networking tool on the Internet, boasts 350 million active users, 175 million of whom sign onto the site every day.

A Facebook user fills out personal information and can allow the program to access their email contacts to connect with other Facebook users. The user can search others by name to find friends, colleagues and associates. If a user isn't able to find a friend on Facebook, they can generate an invitation that is delivered by email.

Facebook users are identified by their real names, which creates an environment of trust, and also allows people to easily find friends. They add details about themselves, families, relationship status, preferences and interests. Users can join groups , which support causes, or are based around common interests. They can become "fans" of businesses or public figures. They can link to news stories, music and video as well as upload pictures and write status updates about their activities.  Any activity a user engages in appears on their friends' *Live Feed*. Friends can comment on one another's activity, reply to threads on their personal feeds, called the *Wall*, and upload their own videos, pictures, music and news articles onto their friends' Walls. Mutual friends see interactions between two users as part of their own News Feed, but others do not. Facebook's privacy settings allow users to customize who can  and cannot see their activities.

Through *Facebook Connect*, users can add updates to their Wall without signing into the actual site. Users of sites like Yelp.com, a popular consumer review site with a focus on local businesses, can choose the option of having all their reviews appear simultaneously on Yelp and Facebook. Similarly, users of the urban adventure site Foursquare.com can post their locations to Facebook, essentially inviting their friends into their game.

As the US intelligence community moves from a need-to-know model to a need-to-share model, a utility that allows members of the community to seamlessly connect with one another, draw information on a push rather than a pull basis, and effortlessly share information without having to actively take steps to do so may be very useful.

An important component of this plan would be linking databases to the *News Feed*. The 16 agencies that make up the US intelligence community all draw upon different databases (some of which have been referred to in the press as "vast data warehouses"). One might reasonably assume that each database has its strengths and weaknesses and that there is some redundancy in the information users pull from them. If the databases were connected to an active News Feed, users of an Intelink social networking site would see when their colleagues accessed, uploaded, or modified items within the databases. If the databases use a controlled vocabulary or user generated tags, keywords could trigger a notification to members of a user group or fan page.

Even if the users who receive the notification do not have access to the database itself, they would have some idea that a certain type of information exists. Because the site would not be anonymous, users would be trading in reputation and skill at tradecraft, and would have incentives to make connections across different agencies with others who could aid in their work, based on their evolving reputations.

Second, and more importantly, an algorithm needs to be created that can compare the contents of databases. While multiple databases might have information on, say, Jane Doe, one might have all her known addresses, educational history and places of work, while another might have recorded information on her habits, public remarks, and purchases at a certain relevant location. Yet a third database might contain observational information on her health. Taken together, one would be able to make better projections about potential threats posed by Jane Doe.

Clearly something must be done to improve data mining standards with the use of more sophisticated data aggregation methods, resource sharing and algorithmic interpretations to not only prevent relevant information from slipping between the cracks, but to take it a step farther and reveal previously overlooked connections. An algorithm would be able to compare the contents of classified databases without compromising the security of the information contained in the database. What it might reveal is that classified data and information are less and less valuable, and that classification and secrecy hinder the flow of information in an age that calls for real time responses.

## Conclusion

The defense intelligence community found Intellipedia, its wiki, enormously useful, at least at the lower levels of the intelligence community. Between 2006 and 2009, it grew from 3,000 active users to 100,000. Security concerns have been addressed by creating three different versions of the wiki, used by groups with different security clearances.

Classified information may become less and less valuable as more information is openly available, through civilian maintained databases, public records, online in the form of social networking status updates, on blogs, in tweets, and elsewhere. The intelligence community must continue its transition from providing information between agencies on a need-to-know basis to a need-to-share basis. A networking utility for the intelligence community that draws upon some of the features of Facebook, along with an algorithm that compares and indexes both open-source and classified databases, may be able to hit the right balance of push-pull intelligence to respond to the constantly changing threat environment in which the intelligence community works.

One benefit of a utility like the one proposed in this paper is that it has a low learning curve, and technology doesn't take the place of smart humans, but rather could serve the function of making those smart humans smarter, faster. Being able to quickly understand the differences in the information contained in different databases would allow members of the intelligence community to make better choices about which databases to draw on, whether the information in classified databases is really more valuable than more readily available information and whether the intelligence community contains gaps that are filled in relevant ways by engaged civilian groups or by publicly available data.

Seeing what others are working on, and being able to quickly communicate across departments or agencies would result in more rapid coalescence of important information in the creation of intelligence products.

### *Bibliography*

Andrus, D. C. (2005). The Wiki and the blog: toward a complex adaptive intelligence community. *Studies in Intelligence*, 49(3), Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904 (2010, February 8)

Baker, P. (2010, January 4). Obama's war over terror. *The New York Times Magazine*, Retrieved from http://www.nytimes.com/2010/01/17/magazine/17Terror-t.html (2010, February 8)

Berkowitz, B. (2007, April 14). *Failing to keep up with the information revolution the DI and "it"*. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article07.html (2010, February 8)

Burke, C. (2007). Freeing knowledge, telling secrets: open source intelligence and development. *Centre for East-West Cultural and Economic Studies*, 11. Retrieved from http://epublications.bond.edu.au/cewces papers/11 (2010, February 8)

Carter, S.A. (1998, December 17). *Pull, push or shove: global broadcast service and intelligence support to maritime forces*. Retrieved from http://www.stormingmedia.us/69/6916/A691663.html (2010, February 8)

Courson, P., & Turnham, S. (2003, July 30). Amid furor, pentagon kills terrorism futures market. *CNN.com*, Retrieved from http://www.cnn.com/2003/ALLPOLITICS/07/29/terror.market/index.html (2010, February 8)

Frakes, W.B., & Baeza_Yates, R. (2004). *Information retrieval: data structures and algorithms*. Retrieved from http://www.scribd.com/doc/13742235/Information-Retrieval-Data-Structures-Algorithms-William-B-Frakes#about (2010, February 8)

French, J.C., Powell, A.L., Callan, J, Viles, C.L., & Emmitt, T. (1999). *Comparing the performance of database selection algorithms*. Retrieved from http://www.cs.virginia.edu/~cyberia/papers/SIGIR99.pdf (2010, February 8)

Jackson, J. (2009, February 18). *Intellipedia suffers midlife crisis*. Retrieved from http://gcn.com/Articles/2009/02/18/Intellipedia.aspx (2010, February 8)

Kanter, R.M. (2010, January 4). *Northwest flight 253's lessons for leaders*. Retrieved from http://blogs.hbr.org/kanter/2010/01/northwest-flight-253s-lessons.html (2010, February 8)

Leiter, M. (2008). An Interagency Threat Assessment Coordination Group (ITACG) Progress Report - Statement for the Record, Michael Leiter, Acting Director, NCTC. *13 March 2008*

*Hearing before the House Homeland Security Committee's Sub-committee on Intelligence, Information Sharing and Terrorism.* Retrieved (2010, February 8)

Miles, D. (2010, February 2). Review calls for stronger cooperation. *American Forces Press Service.* Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=57831 (2010, February 8)

*National counterterrorism center key partners.* (2009, February 13). Retrieved from http://www.nctc.gov/about_us/key_partners.html (2010, February 8)

*NCTC and information sharing, five years since 9/11: a progress report* . (2006, September 01). Retrieved from http://www.nctc.gov/docs/report_card_final.pdf (2010, February 8)

Stern, S. (2010, January 11). A Little knowledge is deadly dangerous. *ft.com*, Retrieved from http://www.ft.com/cms/s/0/baf685ec-fed9-11de-a677-00144feab49a.html?nclick_check=1 (2010, February 8)

Thompson, C. (2006, December 3). Open source spying. *The New York Times Magazine.* Retrieved from http://www.nytimes.com/2006/12/03/magazine/03intelligence.html (2010, February 8)